AMENDMENTS TO THE CLAIMS:

Claims 1-16 and 18-32 are pending in the subject application. It is proposed that claim 30 be amended as set forth herein. Upon entry of these amendments, this Listing of Claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Previously Presented) One or more computer-readable media having computer-executable instructions embodied thereon that, when executed, provide a system that facilitates access to a plurality of shared software objects by disparate entities, the system comprising:

a platform component executed by a computing device having a processor and a memory, that receives a request from a first entity to access one of the plurality of shared software objects, wherein the first entity is attempting to convert a subscription from a second type of a second entity to a first type of the first entity;

a data store that stores security information on one or more classes of the plurality of shared software objects, wherein the security information on each of the one or more classes is inherited by one or more shared software objects in each class, and wherein the security information includes a security parameter that indicates whether the first entity is permitted to convert the subscription from the second type to the first type; and

a verification component that employs the security information to verify that the first entity has permission to call an Application Programming Interface (API) for the one of the plurality of shared software objects to convert the

subscription from the second type to the first type, wherein the verification component prevents the first entity from calling the API when the security parameter indicates that the first entity is not permitted to convert the subscription from the second type to the first type and the verification allows the first entity to call the API when the security parameter indicates that the first entity is permitted to convert the subscription from the second type to the first type.

2. (Previously Presented) The media of claim 1, wherein the verification component exposes the one of the plurality of shared software objects to the entity if permission exists.

3. (Previously Presented) The media of claim 1, wherein the verification component masks the object one of the plurality of shared software objects from the entity if permission does not exist.

4. (Previously Presented) The media of claim 1, wherein the platform component further comprises a Subscription Platform Service to facilitate automated billing and provisioning of accounts.

5. (Previously Presented) The media of claim 1, wherein the verification component facilitates that the entity receive full access to Application Programming Interfaces (APIs) and/or objects for which there is a business need and partial or limited access to other APIs or business objects.

6. (Previously Presented) The media of claim 1, wherein the data store provides default or determined security information related to ~~a class~~ at least a portion of the one or more classes.

7. (Previously Presented) The media of claim 6, wherein the system further comprises a component to override the default security information with higher or different security options.

8. (Previously Presented) The media of claim 1, wherein the system further comprises a proxy tenant component having an intermediate entity that places calls into a subscription platform service on behalf of another entity and achieves access to selected objects of the plurality of shared software objects in order for the another entity to complete a subscription purchase.

9. (Previously Presented) The media of claim 1, wherein the system further comprises a management portal to facilitate authorization of information.

10. (Previously Presented) The media of claim 1, wherein the system further comprises a component to provide an explicit security mapping for one of the plurality of shared software objects.

11. (Previously Presented) The media of claim 1, wherein the system further comprises a component to enable an implicit security mapping from an explicitly mapped one of the plurality of shared software objects or to derive an implied security permission by utilizing related objects of the plurality of shared software objects.

12. (Previously Presented) The media of claim 1, wherein the verification component employs operating system identities to facilitate security authorization procedures.

13. (Previously Presented) The media of claim 1, wherein the system further comprises at least one of a sign-up API caller, an account management API caller, and a customer care API caller.

14. (Previously Presented) The media of claim 13, wherein the system further comprises at least one API related to at least one of a sign-up API group, an account management API group, a customer care API group, and an object designer API group.

15. (Previously Presented) The media of claim 1, wherein the system further comprises authorization logic that determines whether an API can access ~~an object~~ one or more of the plurality of shared software objects via an access rights set.

16. (Previously Presented) The media of claim 1, wherein the system further comprises at least one of a restricted audience offer, a conversion component, and a payment instrument component.

17. (Cancelled).

18. (Previously Presented) A method to facilitate security for subscription objects, comprising:

storing one or more security options in a database, at least a portion of the one or more security options being related to an automated billing and

provisioning system, wherein at least a portion of the one or more security options includes at least conversion of a subscription from a first type associated with a first tenant to a second type associated with a second tenant, and wherein one or more of the security options indicate allowability of the second tenant to convert the subscription type from the first type to the second type;

assigning one or more of the security options to a class; and

inheriting the one or more security options assigned to the class by object members of the class.

19. (Previously Presented) The method of claim 18, further comprising at least one of explicitly and implicitly assigning one or more of the security options to the object members of the class.

20. (Original) The method of claim 18, further comprising accessing the database via an application programming interface (API).

21. (Original) The method of claim 20, further comprising automatically authorizing the API.

22. (Original) The method of claim 21, further comprising returning an error code if an authorization procedure fails.

23. (Original) The method of claim 21, further comprising analyzing a simple object access protocol request.

24. (Original) The method of claim 21, further comprising analyzing one or more security credentials.

25. (Original) The method of claim 24, further comprising employing a cache to process the credentials.

26. (Previously Presented) The method of claim 18, wherein the automated billing and provisioning system further comprises a Subscription Platform Service.

27. (Previously Presented) The method of claim 18, wherein at least a portion of the one or more security options is associated with default security parameters.

28. (Previously Presented) The method of claim 18, further comprising overriding the default security parameters with other security options of the one or more security options.

29. (Original) The method of claim 18, further comprising employing an intermediate proxy that places calls into a subscription platform service on behalf of another tenant.

30. (Currently Amended) One or more computer-readable media having computer-executable instructions embodied thereon that, when executed, provide a [[A]] system ~~embodied on a computer readable storage medium~~ to facilitate business object security, comprising:

an authentication component executing on a computing device having a memory and a processor that authenticates a first entity attempting to access [[to]]

an online billing and service system, wherein the first entity is attempting to convert a subscription from a second type of a second entity to a first type of the first entity;

an authorization component that authorizes the first entity to convert the subscription from the second type of the second entity to the first type of the first entity upon verifying at least one security parameter, wherein the at least one security parameter is assigned to a class of objects and is inherited by objects of the class by one or more of explicitly and implicitly assigning the security parameter to the objects of the class, wherein the at least one security parameter is stored in a database and is accessible via an application program interface that is automatically authorized by analyzing one or more security credentials, and wherein the at least one security parameter indicates allowability of the first entity to convert the subscription from the second type to the first type.

31. (Previously Presented) A computer readable storage medium that stores a data packet that when transmitted facilitates communications between at least two components of a subscription platform service, the data packet comprising:

an Application Programming Interface packet that is executed by a computing device having a processor and a memory to identify a first partner;

a security credential packet to facilitate authorization of the first partner; and

a security parameter packet inherited by a business object to facilitate access to a subscription platform database, wherein the security parameter packet includes at least a security parameter for conversion of a subscription of a

subscriber from a second type associated with a second partner to a first type associated with the first partner, wherein the security parameter indicates allowability of the first partner to convert the subscription from the second type to the first type.

32. (Previously Presented) A computer readable storage medium having a data structure stored thereon, the data structure comprising:

at least one security field indicating global security parameters in a subscription platform database, wherein the global security parameters include at least a security parameter for conversion of a subscription of a subscriber from a first type associated with a first tenant to a second type associated with a second tenant, wherein the security parameter for conversion indicates allowability of the second tenant to convert the subscription from the first type to the second type;

at least one object field associated with an account in the database; and

at least one class field to associate the at least one security field and the at least one object field, wherein an object in the at least one object field that is associated with the at least one class field inherits the at least one security parameter from the at least one class field.